Boletín de diciembre de 2020

Avisos de Sistemas de Control Industrial

Consumo de recursos descontrolado en Touch Panel de las series BTP

Fecha de publicación: 02/12/2020

Importancia: Alta

Recursos afectados:

Todas las versiones de los siguientes productos:

- BTP 2043W (nº 1050387);
- BTP 2070W (nº 1046666);
- BTP 2102W (nº 1046667).

Descripción:

Richard Thomas y Tom Chothia, investigadores de la Universidad de Birmingham, han descubierto una vulnerabilidad, de severidad alta, de tipo consumo descontrolado de recursos, que afecta a varias versiones de las series BTP.

Solución:

Phoenix Contact recomienda utilizar dispositivos con capacidad de red en redes cerradas o protegidos con un *firewall* adecuado. Para obtener información detallada sobre sus recomendaciones de protección de dispositivos con capacidad de red, consultar la siguiente guía.

Detalle:

Cuando el HMI está sujeto, por ejemplo, a una rápida inundación de paquetes ICMP mediante un ataque de denegación de servicio (DoS), el HMI deja de responder a la entrada del usuario y el programa en ejecución no proporciona cambios visuales. Una vez que se detenga el ataque, el HMI volverá a funcionar normalmente. Se ha asignado el identificador CVE-2020-12524 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Vulnerabilidad

Asignación incorrecta de permisos en CompactRIO de National Instruments

Fecha de publicación: 04/12/2020

Importancia: Alta

Recursos afectados:

Driver del controlador CompactRIO, todas las versiones anteriores a 20.5.

Descripción:

Investigadores de Titanium Industrial Security han identificado una vulnerabilidad, de severidad alta, de tipo asignación incorrecta de permisos para recursos críticos, y la han notificado a INCIBE.

Solución:

El fabricante recomienda:

- Actualizar el *driver* del controlador CompactRIO en el *host*, a la versión 20.5.
- Actualizar el *firmware* en los controladores CompactRIO, a la versión 8.5 o superior.
- Formatear el controlador CompactRIO según las indicaciones proporcionadas.
- Repetir los pasos de actualización de *firmware* y formateo para cada equipo en el que se esté ejecutando CompactRIO afectado por la vulnerabilidad.

Detalle:

La asignación incorrecta de permisos se establece por defecto para un punto de entrada de la API de un servicio específico, lo que podría permitir a un usuario no autenticado, reiniciar el controlador de forma remota. Se ha asignado el identificador CVE-2020-25191 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Errores de configuración en dispositivos ABB Arctic wireless gateway

Fecha de publicación: 09/12/2020

Importancia: Media

Recursos afectados:

- ABB Arctic wireless gateway: ARG600/ARC600/ARP600/ARR600 hasta la versión de firmware 3.4.9.
- Viola Systems Arctic gateway en versiones con soporte de interfaz de usuario HTTPS.
- ABB REC/RER 601/603, Viola Systems Arctic wireless gateway en versiones con de interfaz de usuario HTTP y Viola Systems Arctic 3G gateway 2620.

Descripción:

Existe una vulnerabilidad en una configuración por defecto en el firewall incluido en los dispositivos ABB Arctic wireless gateway cuando está habilitada la conexión VPN. En estos casos es posible que equipos conectados ignoren la ruta por defecto configurada en la VPN como "Default route".

Solución:

ABB ha publicado manuales para cambiar la configuración por defecto de estos dispositivos y evitar este error en función de la configuración de cada dispositivo, tanto para una configuración por defecto o puerta de enlace WAN, como una configuración de puerta de enlace VPN con la puerta de enlace WAN, o solo puerta de enlace VPN. Puede consultar cada caso en el siguiente enlace.

Detalle:

El error en la configuración por defecto comunicado por ABB podría permitir a un usuario evadir las políticas de red definidas y usar una puerta de enlace no deseada en los dispositivos conectados a Ethernet en la LAN de Arctic wireless gateway. Se ha asignado el identificador CVE-2020-24684 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, Privacidad, SCADA, SSL/TLS, Vulnerabilidad

---

Múltiples vulnerabilidades en productos Schneider Electric

Fecha de publicación: 09/12/2020

Importancia: Alta

Recursos afectados:

- EcoStruxure™ Control Expert, todas las versiones;
- Unity Pro (antigÃ¤a denominación de EcoStruxure™ Control Expert), todas las versiones;
- EcoStruxure Geo SCADA Expert:
  - 2019: versión original y actualizaciones mensuales hasta septiembre de 2020, desde 81.7268.1 hasta 81.7578.1;
  - 2020: versión original y actualizaciones mensuales hasta septiembre de 2020, desde 83.7551.1 hasta 83.7578.1.
- Modicon, distintos productos y versiones, disponibles en cada sección *Affected Products and Versions* de los enlaces incluidos en las *Referencias*.

Descripción:

Schneider Electric ha publicado múltiples vulnerabilidades, 8 con severidad alta y 4 medias.

Solución:

Seguir las instrucciones de actualización y configuración descritas en la sección Remediation de cada aviso del fabricante. Puede localizarlos en la sección *Referencias*.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- cualquier condición en la que el atacante tenga la capacidad de escribir un valor arbitrario en una ubicación arbitraria (*write-what-where condition*),
- protección de credenciales insuficientes,
- la aplicación web no hace cumplir la autorización apropiada en todos las URL, *scripts* o archivos restringidos (*forced browsing*),
- comprobación incorrecta de condiciones inusuales o excepcionales,
- falta de autenticación para función crítica,
- limitación inadecuada de una ruta a un directorio restringido (*path traversal*),
- restricción inadecuada de las operaciones dentro de los límites de un búfer de memoria.

Para este conjunto de vulnerabilidades se han asignado los siguientes identificadores: CVE-2020-7560, CVE-2020-28219, CVE-2020-7539, CVE-2020-7541, CVE-2020-7540, CVE-2020-7535, CVE-2020-7549, CVE-2020-7536, CVE-2020-7537, CVE-2020-7542, CVE-2020-7543 y CVE-2020-28220.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, SCADA, Schneider Electric, Vulnerabilidad

---

Múltiples vulnerabilidades en la pila TCP/IP implementada en uIP, Contiki-OS, FNET, picoTCP y Nut/OS

Fecha de publicación: 09/12/2020

Importancia: Crítica

Recursos afectados:

Múltiples productos IoT que utilizan alguna de las siguientes librerías para implementar la pila TCP/IP:

- uIP-Contiki-OS, versión 3.0 y anteriores.
- uIP-Contiki-NG, versión 4.5 y anteriores.
- uIP, versión 1.0 y anteriores.
- open-iscsi, versión 2.1.12 y anteriores.
- picoTCP-NG, versión 1.7.0 y anteriores.
- picoTCP, versión 1.7.0 y anteriores.
- FNET, versión 4.6.3.
- Nut/Net, versión 5.1 y anteriores.

Puede consultarse la lista de productos afectados en el siguiente enlace.

Descripción:

Investigadores de Forescout Research Labs informaron del descubrimiento de un total de 33 vulnerabilidades, 3 de riesgo crítico, en las librerías que usan en múltiples dispositivos IoT para la implementación de la pila de comunicaciones TCP/IP.

Las vulnerabilidades encontradas podrían causar fugas de información, denegaciones de servicio, ejecución de código arbitrario o tomar el control de los dispositivos afectados.

Solución:

- FNET recomiendan a los usuarios actualizar a la versión 4.7.0 o posterior.
- uIP-Contiki-NG recomiendan a los usuarios actualizar a la última versión.
- open-iscsi recomiendan a los usuarios actualizar a la última versión.
- picoTCP-NG, debe contactar con encargados de mantenimiento.
- Nut/Net debe contactar con encargados de mantenimiento.

Algunos fabricantes de productos afectados ya han publicado sus respectivas actualizaciones. Puede conocer el detalle en el siguiente enlace.

Detalle:

Las vulnerabilidades descubiertas por Forescout Research Labs permitirían lectura fuera de límites, desbordamiento de enteros, escritura fuera de límites y validación de entradas de manera incorrecta.

Se han asignado los siguientes identificadores para estas vulnerabilidades: CVE-2020-24336, CVE-2020-24338, CVE-2020-25111 (estos 3 primeros son los críticos), CVE-2020-13984, CVE-2020-13985, CVE-2020-13986, CVE-2020-13987, CVE-2020-13988, CVE-2020-17437, CVE-2020-17438, CVE-2020-17439, CVE-2020-17440, CVE-2020-17441, CVE-2020-17442, CVE-2020-17443, CVE-2020-17444, CVE-2020-17445, CVE-2020-17467, CVE-2020-17468, CVE-2020-17469, CVE-2020-17470, CVE-2020-24334, CVE-2020-24337, CVE-2020-24339, CVE-2020-24340, CVE-2020-24340, CVE-2020-24341, CVE-2020-24383, CVE-2020-25107, CVE-2020-25108, CVE-2020-25109, CVE-2020-25110 y CVE-2020-25112.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, IoT, SCADA, Vulnerabilidad

---

Avisos de seguridad de Siemens de diciembre de 2020

Fecha de publicación: 09/12/2020

Importancia: Crítica

Recursos afectados:

- SENTRON PAC3200, versiones 2.4.5 y anteriores;
- SENTRON PAC4200: versiones 2.0.1 y anteriores;
- SIRIUS 3RW5 módulo de comunicación Modbus TCP, todas las versiones;
- XHQ Operations Intelligence, todas las versiones anteriores a 6.1;
- SICAM A8000 CP-8000, todas las versiones anteriores a la 16;
- SICAM A8000 CP-8021, todas las versiones anteriores a la 16;
- SICAM A8000 CP-8022, todas las versiones anteriores a la 16;
- SIMATIC, distintas versiones disponibles en el apartado 3.1 de los avisos ICSA-20-343-08 e ICSA-20-343-09;
- LOGO! 8 BM (incluye variantes de SIPLUS), todas las versiones anteriores a 8.3;
- LOGO! Soft Comfort, todas las versiones anteriores a 8.3 (solo afectadas por las vulnerabilidades CVE-2020-25231 y CVE-2020-25234).

Descripción:

Siemens ha publicado en su comunicado mensual varias actualizaciones de seguridad de diferentes productos.

Solución:

Acceder a la sección *4. MITIGATIONS* de los avisos del CISA y/o a la columna *Remediation* en las tablas de los PDF de Siemens para obtener las soluciones a estas vulnerabilidades.

Detalle:

Siemens, en su comunicación mensual de parches de seguridad, ha emitido un total de 24 avisos de seguridad, de los cuales 18 son actualizaciones de avisos publicados anteriormente.

Los tipos de nuevas vulnerabilidades publicadas se corresponden con los siguientes:

- desbordamiento de enteros,
- exposición de información sensible a usuarios no autorizados,
- XSS,
- XSS básico,
- inyección SQL,
- limitación inadecuada de una ruta relativa a un directorio restringido (*relative path traversal*),
- CSRF,
- fallo en mecanismo de protección,
- desbordamiento de búfer basado en montículo (*heap*),
- desreferencia a puntero nulo,
- desbordamiento de búfer,
- excepción no controlada,
- falta de autenticación en función crítica,
- uso de claves criptográficas en claro,
- algoritmo de cifrado débil o directamente vulnerable,
- credenciales insuficientemente protegidas.

Para estas vulnerabilidades se han asignado los siguientes identificadores: CVE-2020-13988, CVE-2019-19283, CVE-2019-19284, CVE-2019-19285, CVE-2019-19286, CVE-2019-19287, CVE-2019-19288, CVE-2019-19289, CVE-2020-28396, CVE-2019-15678, CVE-2019-15679, CVE-2019-15680, CVE-2019-8287, CVE-2020-15796, CVE-2020-25228, CVE-2020-25229, CVE-2020-25230, CVE-2020-25231, CVE-2020-25232, CVE-2020-25233, CVE-2020-25234 y CVE-2020-25235.

Etiquetas: Actualización, Infraestructuras críticas, Siemens, Vulnerabilidad

---

Múltiples vulnerabilidades en productos GE Healthcare

Fecha de publicación: 09/12/2020

Importancia: Crítica

Recursos afectados:

Múltiples dispositivos IoT de imagen y ultrasonido de GE Healthcare. Las versiones afectadas se pueden consultar en el portal web de GE y el aviso del CISA ICSMA-20-343-01

Descripción:

Lior Bar Yosef y Elad Luz, investigadores de CyberMDX, han informado de dos vulnerabilidades, ambas de severidad crítica, de tipo pérdida de autenticación y exposición de información sensible a una esfera de control no autorizada.

Solución:

GE recomienda consultar su portal web para obtener detalles sobre las mitigaciones y medidas proactivas a aplicar para cada

producto afectado. Las medidas proactivas garantizarán la protección del firewall de cada producto y se modificarán las contraseñas predeterminadas.

Detalle:

La explotación de estas vulnerabilidades podría permitir a un atacante, con acceso a la red corporativa de prestación de servicios médicos, obtener acceso a los dispositivos afectados de forma remota, exponer o modificar datos confidenciales, o afectar a la disponibilidad del sistema. Se han asignado los identificadores CVE-2020-25175 y CVE-2020-25179 para cada vulnerabilidad respectivamente.

Etiquetas: Comunicaciones, Infraestructuras críticas, IoT, Sanidad, Vulnerabilidad

---

Vulnerabilidad de lectura fuera de límites en productos Mitsubishi Electric

Fecha de publicación: 09/12/2020

Importancia: Alta

Recursos afectados:

- GT2107-WTBD, todas las versiones;
- GT2107-WTSD, todas las versiones;
- GT2104-RTBD, todas las versiones;
- GT2104-PMBD, todas las versiones;
- GT2103-PMBD, todas las versiones;
- GS2110-WTBD, todas las versiones;
- GS2107-WTBD, todas las versiones;
- LE7-40GU-L, todas las versiones.

Descripción:

Se ha identificado una vulnerabilidad, de severidad alta, de tipo lectura fuera de límites.

Solución:

Mitsubishi Electric recomienda restringir el acceso a los productos afectados sólo desde redes y hosts de confianza hasta que se publiquen las actualizaciones respectivas.

Detalle:

La vulnerabilidad de lectura fuera de límites podría permitir a un atacante remoto degradar el rendimiento de una comunicación o provocar una condición de denegación de servicio (DoS) de las funciones de comunicación TCP de los productos afectados, mediante el envío de paquetes especialmente diseñados. Se ha asignado el identificador CVE-2020-5675 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de gestión inadecuada de condiciones excepcionales en Mitsubishi Electric MELSEC iQ-F Series

Fecha de publicación: 11/12/2020

Importancia: Alta

Recursos afectados:

MELSEC iQ-F series, versión 1.060 y anteriores del módulo de CPU FX5U(C).

Descripción:

El fabricante afectado ha reportado una vulnerabilidad, de severidad alta, de tipo comprobación o gestión inadecuada de condiciones excepcionales.

Solución:

Actualizar el *firmware* del producto afectado a la versión 1.061 o posteriores.

Detalle:

En los módulos de la serie iQ-F de MELSEC existe una vulnerabilidad de comprobación o gestión inadecuada de las condiciones excepcionales, que podría dar lugar a una condición de denegación de servicio (DoS), y que requeriría de un reinicio del módulo de la CPU para su recuperación. Se ha asignado el identificador CVE-2020-5665 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de validación de entrada incorrecta en ECOM100 Module de Host Engineering

Fecha de publicación: 11/12/2020

Importancia: Alta

Recursos afectados:

- H0-ECOM100 Module:
  - versiones de *hardware* 6x y anteriores con versiones de *firmware* 4.0.348 y anteriores;
  - versiones de *hardware* 7x con versiones de *firmware* 4.1.113 y anteriores;
  - versiones de *hardware* 9x con versiones de *firmware* 5.0.149 y anteriores.
- H2-ECOM100 Module:
  - versiones de *hardware* 5x y anteriores con versiones de *firmware* 4.0.2148 y anteriores;
  - versiones de *hardware* 8x con versiones de *firmware* 5.0.1043 y anteriores.
- H4-ECOM100 Module: versiones de *firmware* 4.0.2148 y anteriores,

Los productos sólo son vulnerables si el servidor web está habilitado, y está desactivado por defecto.

Descripción:

Uri Katz, investigador de Claroty, ha reportado una vulnerabilidad, de severidad alta, de tipo validación de entrada incorrecta.

Solución:

Host Engineering recomienda a los usuarios que actualicen los dispositivos de campo afectados utilizando *Live Update* en su *software* NetEdit3. Además, el fabricante recomienda que si los productos afectados no pueden ser actualizados, la desactivación del servidor web sirve como una solución alternativa.

Detalle:

La longitud de los campos de entrada del producto afectado sólo se verifica en el lado del cliente cuando se reciben los datos de entrada del servidor web de configuración, lo que podría permitir a un atacante eludir dicha comprobación y enviar datos de entrada para bloquear el dispositivo. Se ha asignado el identificador CVE-2020-25195 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

Múltiples vulnerabilidades en Medtronic MyCareLink Smart

Fecha de publicación: 11/12/2020

Importancia: Alta

Recursos afectados:

MyCareLink (MCL) Smart Model 25000 Patient Reader, todas las versiones.

Descripción:

Diversos investigadores han notificado a Medtronic 3 vulnerabilidades de severidad alta, de tipo autenticación inadecuada, desbordamiento de búfer basado en memoria dinámica (*heap*) y condición de carrera TOCTOU.

Solución:

- Acceder a la tienda de aplicaciones móviles asociada y actualizar MyCareLink Smartapp a la versión *firmware* 5.2.
- Actualizar la versión del sistema operativo del dispositivo móvil a iOS 10 o superior, o Android 6.0 o superior.

Detalle:

- La vulnerabilidad de autenticación inadecuada por omisión, que radica en el protocolo de autenticación entre MCL Smart Patient Reader y la app móvil MyCareLink Smart, podría permitir a un atacante realizar un *spoofing* contra el MCL Smart Patient Reader dentro del rango de alcance de la comunicación Bluetooth. Se ha asignado el identificador CVE-2020-25183 para esta vulnerabilidad.
- La vulnerabilidad de desbordamiento de búfer basado en memoria dinámica podría permitir a un atacante ejecutar código de forma remota en MCL Smart Patient Reader, pudiendo resultar en el control del dispositivo. Se ha asignado el identificador CVE-2020-25187 para esta vulnerabilidad.
- La vulnerabilidad de condición de carrera TOCTOU afecta al sistema de actualización del *software* MCL Smart Patient Reader y podría permitir a un atacante cargar y ejecutar *firmware* sin firmar, dando lugar a la ejecución remota de código y el control del dispositivo. Se ha asignado el identificador CVE-2020-27252 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Sanidad, Vulnerabilidad

Múltiples vulnerabilidades en productos de ABB

Fecha de publicación: 16/12/2020

Importancia: Crítica

Recursos afectados:

- ABB Ability™ Symphony®Plus:
  - S Operations 1.1;
  - S Operations 2.0, todos los Service Packs;
  - S Operations 2.1, Service Pack 1 (SP1), para Melody y otros Heritage systems;
  - S Operations 2.1, Service Pack 2 (SP2);
  - S Operations 3.0;
  - S Operations 3.1;
  - S Operations 3.2;
  - S Operations 3.3.
- ABB Ability™ Symphony®Plus:
  - S Historian 3.0 y 3.1.
- ABB Central Licensing System (CLS) en ABB Ability™ Symphony Plus Operations (desde la 3.0 hasta la 3.3);
- ABB Central Licensing System (CLS) en ABB Ability™ Symphony Plus Engineering (desde la 1.0 hasta la 2.3);
- ABB Central Licensing System (CLS) en Composer Harmony (5.1, 6.0 y 6.1);
- ABB Central Licensing System (CLS) en Composer Melody (5.3 y 6.1);
- ABB Central Licensing System (CLS) en HarmonyOPC Server (6.0, 6.1 y 7.0).

Descripción:

ABB ha publicado múltiples vulnerabilidades que podrían permitir a un atacante abusar de las funcionalidades de los productos afectados.

Solución:

- Para S Operations:
  - Actualizar a la versión 3.3 Service Pack 1.
- Para S Operations, versiones anteriores a la 3.X, se preveen tres actualizaciones:
  - Q4 2020: S Operations 2.1 SP 2 Rollup 2 (Harmony, SD y Freelance);
  - Q1 2021: S Operations 2.2 (Melody y Procontrol P14);
  - Q3 2021: S Operations 2.2 Rollup 1 (Procontrol P13).
- Para ABB Ability™ Symphony®Plus:
  - Actualizar a S Historian 3.2.
- Para Sym-phony Plus, Composer Harmony, Composer Melody y HarmonyOPC Server:
  - Actualizar a la última versión disponible y aplicar las medidas de seguridad genéricas, descritas en el aviso 2PAA121231.

Detalle:

- Las vulnerabilidades críticas que afectan al producto ABB Ability™ Symphony®Plus Operations y ABB Ability™ Symphony®Plus Historian, son del tipo:
  - SQL Injection. Se ha asignado el identificador CVE-2020-24673 para esta vulnerabilidad.
  - Método de autenticación débil. Se ha asignado el identificador CVE-2020-24675 para esta vulnerabilidad.
  - Omisión de autenticación. Solo afecta a S Operations. Se ha asignado el identificador CVE-2020-24683 para esta vulnerabilidad.
- Las vulnerabilidades críticas que afectan a los productos Sym-phony Plus, Composer Harmony, Composer Melody y HarmonyOPC Server, son del tipo:
  - XXE. Se ha asignado el identificador CVE-2020-8479 para esta vulnerabilidad.
  - Divulgación de información. Se ha asignado el identificador CVE-2020-8481 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-24674, CVE-2020-24676, CVE-2020-24677, CVE-2020-24678, CVE-2020-24679, CVE-2020-24680, CVE-2020-8481 y CVE-2020-8471.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de Phoenix Contact

Fecha de publicación: 17/12/2020

Importancia: Alta

Recursos afectados:

- Versiones anteriores a la 8.8.3 de los productos:
  - TC MGUARD RS4000 4G VZW VPN,
  - TC MGUARD RS4000 4G ATT VPN,
  - FL MGUARD RS4004 TX/DTX,
  - FL MGUARD RS4004 TX/DTX VPN,
  - TC MGUARD RS4000 3G VPN,
  - TC MGUARD RS4000 4G VPN ,
  - Innominate mGuard rs4000 4TX/TX,
  - Innominate mGuard rs4000 4TX/TX VPN,
  - Innominate mGuard rs4000 4TX/3G/TX VPN.
- Versiones anteriores a 2021.0 LTS de los productos:
  - AXC F 1152,
  - AXC F 2152,

- AXC F 3152,
- RFC 4072S,
- AXC F 2152 Starterkit,
- PLCnext Technology Starterkit.

Descripción:

El equipo de SMST Designers & Constructors B.V y diversos investigadores de SVA Systemvertrieb Alexander GmbH han descubierto 5 vulnerabilidades, 2 con severidad alta y 3 medias, que afectan a múltiples productos de Phoenix Contact.

Solución:

En el apartado *Affected products* de cada aviso del apartado referencias, aplicar las actualizaciones disponibles para su descarga en la columna *Fixed Version* de cada producto afectado.

Detalle:

- Los parámetros HTTP de los interfaces web no sanitizan adecuadamente las entradas de datos, lo que podría ocasionar un ataque XSS almacenado. Se ha asignado el identificador CVE-2020-12517 para esta vulnerabilidad de severidad alta.
- Una cuenta de sistema, sin privilegios de acceso, podría ser utilizada para ejecutar comandos de *shell* con privilegios de *root*, que podrían permitir al atacante obtener acceso *root*. Se ha asignado el identificador CVE-2020-12519 para esta vulnerabilidad de severidad alta.
- Un atacante podría utilizar los conocimientos adquiridos, mediante la lectura de la información sensible insuficientemente protegida, para planificar nuevos ataques. Se ha asignado el identificador CVE-2020-12518 para esta vulnerabilidad de severidad media.
- Un paquete de LLDP, especialmente diseñado, podría llevar a una alta carga del sistema en la pila PROFINET, pudiendo causar un fallo en los servicios del sistema o un reinicio completo. Se ha asignado el identificador CVE-2020-12521 para esta vulnerabilidad de severidad media.
- Para los dispositivos mGuard con *switch* integrado en la LAN, los puertos de un solo interruptor pueden ser desactivados en la configuración del dispositivo. Después de un reinicio, estos puertos se ponen en funcionamiento independientemente de su configuración. Un atacante podría acceder a datos confidenciales o poner en peligro la disponibilidad de los servicios mGuard mediante la inundación (*flooding*) o el agotamiento de los recursos. Se ha asignado el identificador CVE-2020-12523 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Vulnerabilidad de permisos predeterminados incorrectos en Kepware LinkMaster Service

Fecha de publicación: 17/12/2020

Importancia: Crítica

Recursos afectados:

Kepware LinkMaster, versión 3.0.94.0.

Descripción:

El investigador Yuri Kramarz de Cisco Talos ha reportado una vulnerabilidad, de severidad crítica, de tipo permisos predeterminados incorrectos.

Solución:

Por el momento, el fabricante no ha proporcionado una solución para esta vulnerabilidad.

Detalle:

Un atacante local podría modificar la configuración del archivo binario existente para ejecutar código arbitrario con privilegios de NT SYSTEM, aprovechando la vulnerabilidad de permisos predeterminados incorrectos en LinkMasterV3 Service. Esta podría permitir una escalada de privilegios a cualquier usuario. Se ha asignado el identificador CVE-2020-13535 para esta vulnerabilidad.

Etiquetas: Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Inyección de comandos en varios productos de WAGO

Fecha de publicación: 18/12/2020

Importancia: Crítica

Recursos afectados:

Todas las versiones de *firmware* 10 y anteriores de los siguientes productos:

- Series PFC100 (750-81xx/xxx-xxx);
- Series PFC200 (750-82xx/xxx-xxx);

- Series Wago Touch Panel 600 Standard Line (762-4xxx);
- Series Wago Touch Panel 600 Advanced Line (762-5xxx);
- Series Wago Touch Panel 600 Marine Line (762-6xxx).

Descripción:

Florian Seidel, investigador de WAGO, y posteriormente Uri Katz, investigador de Claroty, ambos coordinados por el , han identificado múltiples vulnerabilidades en distintos productos de WAGO.

Solución:

La vulnerabilidad fue solucionada con la publicación, en diciembre de 2017, de la versión 11 del *firmware*.

Detalle:

El servicio I/O-Check contiene una vulnerabilidad que podría permitir a un atacante, que tuviese acceso a la red del dispositivo y por medio de paquetes especialmente diseñados, ejecutar código e incluso manipular o interrumpir el normal funcionamiento del dispositivo. Se ha asignado el identificador CVE-2020-12522 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, Vulnerabilidad

---

Autenticación inapropiada en productos Emerson

Fecha de publicación: 18/12/2020

Importancia: Alta

Recursos afectados:

- X-STREAM enhanced XEGP, todas las versiones;
- X-STREAM enhanced XEGK, todas las versiones;
- X-STREAM enhanced XEFD, todas las versiones;
- X-STREAM enhanced XEXF, todas las versiones.

Descripción:

Maxim Rupp ha informado al CISA de una vulnerabilidad en productos Emerson, de severidad alta, del tipo autenticación inapropiada, que podría permitir a un atacante la divulgación de información.

Solución:

Emerson recomienda a los usuarios que actualicen el *firmware* de los productos afectados. Para más información sobre cómo obtener la actualización, contactar con .

Detalle:

Una autenticación inadecuada en el acceso a los datos de registro y de copia de seguridad podría permitir a un atacante, por medio de una URL especialmente diseñada, descargar ficheros y obtener acceso a información sensible. Se ha asignado el identificador CVE-2020-27254 para esta vulnerabilidad.

Etiquetas: Actualización, Infraestructuras críticas, Vulnerabilidad

---

Multiples vulnerabilidades en PTC Kepware KEPServerEX

Fecha de publicación: 18/12/2020

Importancia: Crítica

Recursos afectados:

Las vulnerabilidades encontradas en la plataforma de conectividad Kepware KEPServerEX, afectan a:

- KEPServerEX: versiones 6.0 a 6.9.
- ThingWorx Kepware Server: versiones 6.8 y 6.9.
- ThingWorx Industrial Connectivity: todas las versiones.
- Agregador OPC: todas las versiones.

Los siguientes productos pueden tener un componente vulnerable:

- Rockwell Automation KEPServer Enterprise.
- GE Digital Industrial Gateway Server: versiones 7.68.804 y 7.66.
- Servidor TOP de Software Toolbox: Todas las versiones 6.x.

Descripción:

El investigador, Uri Katz de Claroty, ha descubierto diferentes vulnerabilidades en productos de la plataforma de conectividad Kepware KEPServerEX que permitirían a un atacante remoto causar una de denegación de servicio, la fuga de datos o ejecución remota de código.

Solución:

PTC ha publicado actualizaciones:

- KEPServerEX:
  - La versión 6.6 debería actualizarse a la versión 6.6.362.0.
  - La versión 6.7 debería actualizarse a la versión 6.7.1067.0.
  - La versión 6.8 debería actualizarse a la versión 6.8.838.0.
  - La versión 6.9 debería actualizarse a la versión 6.9.584.0.
- ThingWorx Kepware Server:
  - La versión 6.8 debería actualizarse a la versión 6.8.839.0.
  - La versión 6.9 debería actualizarse a la versión 6.9.584.0.
- ThingWorx Industrial Connectivity:
  - La versión 8.4 debería actualizarse a la versión 8.4 (6.6.362.0).
  - La versión 8.5 debería actualizarse a la versión 8.4 (6.7.1068.0).
- OPC-Aggregator:
  - La versión 6.9 debería actualizarse a la versión 6.9.584.0.
- Software Toolbox TOP Server:
  - La versión 6.7 debería actualizarse a la versión 6.7.1068.0.
  - La versión 6.8 debería actualizarse a la versión 6.8.840.0.
  - La versión 6.9 debería actualizarse a la versión 6.9.584.0.
- Software Toolbox ha publicado actualizaciones y recomienda a los usuarios que actualicen sus instalaciones.

PTC recomienda actualizar los siguientes productos a la versión compatible más actual:

- Rockwell Automation KEPServer Enterprise.
- GE Digital Industrial Gateway Server:
  - las versiones 7.68.804 y 7.66 deberían actualizarse a la versión 7.68.839.0.

Detalle:

Las vulnerabilidades encontradas permitirían realizar ataques de desbordamiento de búfer basado en la pila, desbordamiento de búfer basado en heap o uso después de la liberación. Siendo las más críticas el desbordamiento de búfer basado en la pila que permitiría abrir un mensaje OPC UA específicamente diseñado y podría bloquear el servidor y ejecutar código de forma remota, y el desbordamiento de búfer basado en heap que permitiría a un atacante bloquear el servidor y potencialmente filtrar datos, también al abrir un mensaje OPC UA, específicamente diseñado.

Se han asignado los identificadores CVE-2020-27265 y CVE-2020-27263 para estas vulnerabilidades y el CVE-2020-27267 para una vulnerabilidad de criticidad alta.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, SCADA, Vulnerabilidad

---

Múltiples vulnerabilidades en Treck TCP/IP stack

Fecha de publicación: 21/12/2020

Importancia: Crítica

Recursos afectados:

Los siguientes componentes de Treck TCP/IP stack, versión 6.0.1.67, están afectados:

- HTTP Server
- IPv6
- DHCPv6

Los productos de algunos fabricantes se ven afectados por estas vulnerabilidades:

- Schneider Electric:
  - TM3 Bus Coupler, EIP *firmware* versión 2.1.50.2 y anteriores;
  - TM3 Bus Coupler, SL *firmware* version 2.0.50.2 y anteriores;
  - TM3 Bus Coupler, CANOpen *firmware* versión 2.0.50.2 y anteriores;
  - TM3 Bus Coupler EIP, *firmware* V2.1.50.2;
  - ATV6000 Medium Voltage Altivar Process Drives, todas las versiones;
  - eIFE Ethernet Interface para MasterPact MTZ, todas las versiones;
  - IFE Ethernet Interface for ComPact, PowerPact, and MasterPact, todas las versiones;
  - IFE GatewayAll versions Acti9 Smartlink IP, todas las versiones;
  - Acti9 PowerTag Link / HD, todas las versiones;
  - Acti9 Smartlink SI D, todas las versiones;
  - Acti9 Smartlink SI B, todas las versiones;
  - EGX150/Link150 Ethernet Gateway, todas las versiones.

Descripción:

Intel, ha reportados estas vulnerabilidades a Treck, de severidades crítica, alta, media y baja, que podrían permitir a un atacante la ejecución remota de código o la denegación de servicio.

Solución:

- Actualizar a la versión Treck TCP/IP 6.0.1.68 o posterior. Las actualizaciones se pueden obtener a través de la dirección de correo .
- Para las soluciones propias de los productos de Schneider Electric, consulte la sección de *Referencias*.

Detalle:

- Una vulnerabilidad de desbordamiento del búfer en la región *heap* de la memoria, en los componentes del Servidor HTTP Treck, podría permitir a un atacante causar la denegación de servicio o la ejecución arbitraria de código. Se ha

asignado el identificador CVE-2020-25066 para esta vulnerabilidad de severidad crítica.
- Una escritura fuera de límites en el componente IPv6 podría permitir a un atacante, no autenticado, la denegación de servicio a través del acceso a la red. Se ha asignado el identificador CVE-2020-27337 para esta vulnerabilidad de severidad alta.
- La lectura fuera de límites, en el componente cliente DHCPv6, podría permitir a un atacante la denegación del servicio a través del acceso a la red adyacente. Se ha asignado el identificador CVE-2020-27338 para esta vulnerabilidad de severidad media.
- La validación incorrecta de la entrada, en el componente IPv6, podría permitir a un atacante, no autenticado, provocar una lectura fuera de límites de hasta 3 bytes mediante el acceso a la red. Se ha asignado el identificador CVE-2020-27336 para esta vulnerabilidad de severidad baja.

Etiquetas: Actualización, Comunicaciones, Infraestructuras críticas, IoT, Schneider Electric, Vulnerabilidad

---

Múltiples vulnerabilidades en Secomea GateManager

Fecha de publicación: 21/12/2020

Importancia: Media

Recursos afectados:

- GateManager 8250, todas las versiones anteriores a la 9.3;
- GateManager 4250/4260/9250, todas las versiones.

Descripción:

Tenable ha informado de una vulnerabilidad de severidad baja y una vulnerabilidad de severidad media, de los tipos XSS almacenado e inyección en el encabezado del *host* en solicitudes HTTP.

Solución:

Actualizar GateManager 8250 a la versión 9.3. Para más detalles, consultar la web de Secomea.

Detalle:

La validación incorrecta de los encabezados HTTP Host, podría permitir a un atacante la inyección de encabezados especialmente diseñados, mediante el envenenamiento de caché. Se ha asignado el identificador CVE-2020-29022 para esta vulnerabilidad.

Para la vulnerabilidad de severidad baja se ha asignado el identificador CVE-2020-29021.

Etiquetas: Actualización, Comunicaciones, IoT, Vulnerabilidad

---

Múltiples vulnerabilidades en Rockwell Automation FactoryTalk

Fecha de publicación: 29/12/2020

Importancia: Alta

Recursos afectados:

- FactoryTalk Linx, versiones 6.00, 6.10, 6.11 y 6.20;
- FactoryTalk Diagnostics, versión 6.11.

Descripción:

Tenable ha reportado a Rockwell Automation 2 vulnerabilidades de severidad alta y 2 de severidad media, siendo las de severidad alta de tipo excepción no controlada.

Solución:

Por el momento no existe solución para estas vulnerabilidades. Los clientes pueden seguir las medidas de mitigación ofrecidas por el fabricante en su web.

Detalle:

- Al procesar los mensajes de OpenNamespace, un atacante remoto, no autenticado, podría enviar una petición especialmente diseñada y bloquear el servicio RSLinxNG.exe, lo que resultaría en una denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-5801 para esta vulnerabilidad.
- Un atacante remoto podría enviar un mensaje *ConfigureItems* especialmente diseñado, al puerto TCP 4241, para bloquear el servicio RSLinxNG.exe, lo que resultaría en una denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-2802.

Para las vulnerabilidades de severidad media se han asignado los identificadores CVE-2020-5806 y CVE-2020-5807.

Etiquetas: Infraestructuras críticas, IoT, Vulnerabilidad